

**FILED**

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

**UNITED STATES DISTRICT COURT  
LAS CRUCES, NEW MEXICO****UNITED STATES DISTRICT COURT**  
for the  
District of New Mexico**JUN 20 2024****MITCHELL R. ELFERS  
CLERK OF COURT**

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 416 Atlas Street, White Sands Missile Range, NM 88002

Case No.

**24-1180 MR****APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See attachment A, attached hereto and incorporated herein.

located in the District of New Mexico there is now concealed (*identify the person or describe the property to be seized*):

See attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

18 U.S.C. § 115(a)(1)(B)

Threats against current and former federal employees and their family members

The application is based on these facts:

See attached Attachment C Affidavit in Support of an Application for a Search Warrant, attached hereto and incorporated herein.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (*give exact ending date if more than 30 days*: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Danielle Oriatti, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
 submitted electronically and sworn telephonically

(specify reliable electronic means).

Date: **6/20/24**

City and state:

**LAS CRUCES, NM**

Judge's signature

**G.J. Fournier, U.S. Magistrate Judge**

Printed name and title



**ATTACHMENT A**

***Property to be searched***

416 Atlas Street, White Sands Missile Range, NM 88002, more particularly described below.

The premises is a one-story single-family residence tan in color with a white color security door in front of the front door. The house number, 416, is listed on the front of the house near the left of the front door.



Biometric Access to Device: During the execution of the search of the PREMISIS described herein, law enforcement officers are also specifically authorized to compel Joseph Rose to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of any device which law enforcement officers are authorized to seize in the scope of this warrant. This warrant does not authorize law enforcement personnel to request that the subject state or otherwise

provide the password or any other means that may be used to unlock or access another person's device, including by identifying specific biometric characteristics, including unique fingers or other physical features that may be used to unlock or access the device.

ATTACHMENT B

*Property to be seized*

All records, information, and evidence relating to violations of 18 U.S.C. § 115(a)(1)(B) involving Joseph Rose, including:

1. Joseph Rose, a person to be arrested;
2. Computers or electronic devices (hereinafter THE DEVICES) that may have been used by Joseph Rose to access Facebook
3. All records or information, contained in or on THE DEVICES, in whatever form they may be found, relating to violations of 18 U.S.C. § 115(a)(1)(B), those violations involving herein named and entities as of yet unknown to us, including:
  - a. All records, documents, materials, notes, and communications related to the use of THE DEVICES to facilitate violations of 18 U.S.C. § 115(a)(1)(B)
  - b. All records, e-mails, text messages, or other communications between subjects known and unknown to us related to schemes in violation of 18 U.S.C. § 115(a)(1)(B).
  - c. evidence of who used, owned, or controlled THE DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - d. evidence of software that would allow others to control THE DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - e. evidence of the lack of such malicious software;
  - f. evidence indicating how and when THE DEVICES were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the computer user;
  - g. evidence indicating THE DEVICES user's state of mind as it relates to the crime under investigation;
  - h. evidence of the attachment to THE DEVICES of other storage devices or similar containers for electronic evidence;



- i. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from THE DEVICES;
- j. evidence of the times THE DEVICES were used;
- k. passwords, encryption keys, and other access devices that may be necessary to access THE DEVICES;
- l. documentation and manuals that may be necessary to access THE DEVICES or to conduct a forensic examination of THE DEVICES;
- m. records of or information about Internet Protocol addresses used by THE DEVICES;
- n. records of or information about THE DEVICE'S Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- o. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:  
416 Atlas Street, White Sands Missile Range,  
NM 88002

Case No.

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Danielle Oriatti, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of criminal Procedure for a warrant to search the premises known as 416 Atlas Street, White Sands Missile Range, NM 88002, herein after the PREMISES, further described in Attachment A, for the things described in Attachment B.
2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since October 2023. I am currently assigned to the Albuquerque Field Office, Las Cruces Resident Agency. During my tenure with the FBI, I have received formal and informal training in conducting a variety of criminal investigations. I have participated in investigations pertaining but not limited to interstate threatening communications and violent crimes. I have executed or participated in the execution of search and arrest warrants. My investigative training and experience include, but is not limited to, conducting surveillance, interviewing subjects, witnesses, and victims, managing cooperating sources, issuing subpoenas, and analyzing records.
3. Through my training, experience, and discussions with other law enforcement officers who have extensive experience in similar investigations, I have become familiar with the tactics and methods used by criminals engaging in various violations of federal law. As a Special Agent, I am authorized to investigate violation of laws of the Unites States, and as a law

enforcement officer, I am authorized to execute warrants issued under the authority of the United States. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 115(a)(1)(B), and I am authorized by the Attorney General to request a search warrant.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit is personally known to me based on my training and experience, was gathered or revealed to me personally during the course of this investigation, or was gathered or revealed to other sworn law enforcement officers during the course of this investigation and subsequently communicated to me.

5. Based on the information set forth herein, there is probable cause to believe that violations of 18 U.S.C. § 115(a)(1)(B) (Threats against current and former federal employees and their family members) were committed, and that evidence of these violations may be found within THE PREMISES.

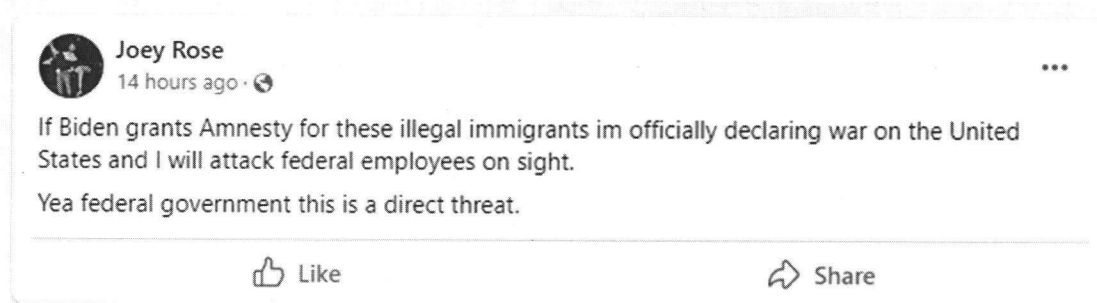
#### PROBABLE CAUSE

##### *Background & Terms*

6. On June 19, 2024, I received information from Army Criminal Investigative Division (CID) of a threat directed towards federal employees through a Facebook post. A government employee and acquaintance of the account holder, Joey Rose, reported the concerning post to Army CID. On that same date, I viewed a copy of the Facebook post, and observed that the post stated, [sic] "If Biden grants Amnesty for these illegal immigrants im officially declaring war on the United States and I will attack federal employees on sight. Yea federal government this is a direct threat." I noted that this post came from a Facebook account



with the name “Joey Rose” and Facebook account identifier “Joey.Rose.77” on June 18, 2024, at 9:15p.m. I also noted that President Biden announced on June 18, 2024, plans for a new program aimed at helping some migrant families stay together by allowing noncitizen spouses and children to apply for lawful permanent residency without leaving the country.



7. On the same date, Army CID ran database checks on Joseph Rose. Army CID identified that Joseph Rose is a medically retired United States Marine veteran and identified the PREMISES on White Sands Missile Range in New Mexico as his current address.

8. On June 19, 2024, Army CID agents requested that Meta Platforms Inc. voluntarily disclose, pursuant 18 U.S.C. § 2702, subscriber information for the Facebook account Joey.Rose.77. Meta Platforms, Inc. disclosed subscriber information for the Facebook account Joey.Rose.77, to include verified a cell phone number 210-913-9272 and Internet Protocol address (IP address) 2601:08c1:8280:5500:a5ad:d263:1277:79a5, 2024-06-17 06:31:39 UTC.

9. On the same date, Army CID agents and FBI agents requested that AT&T voluntarily disclose, pursuant 18 U.S.C. § 2702 cell phone location data for phone number 210-913-9272. I noted cell phone location data from the timing advance and up to June 20, 2024, showed the cell phone location near the PREMISES on White Sands Missile Range that was identified by Army CID.

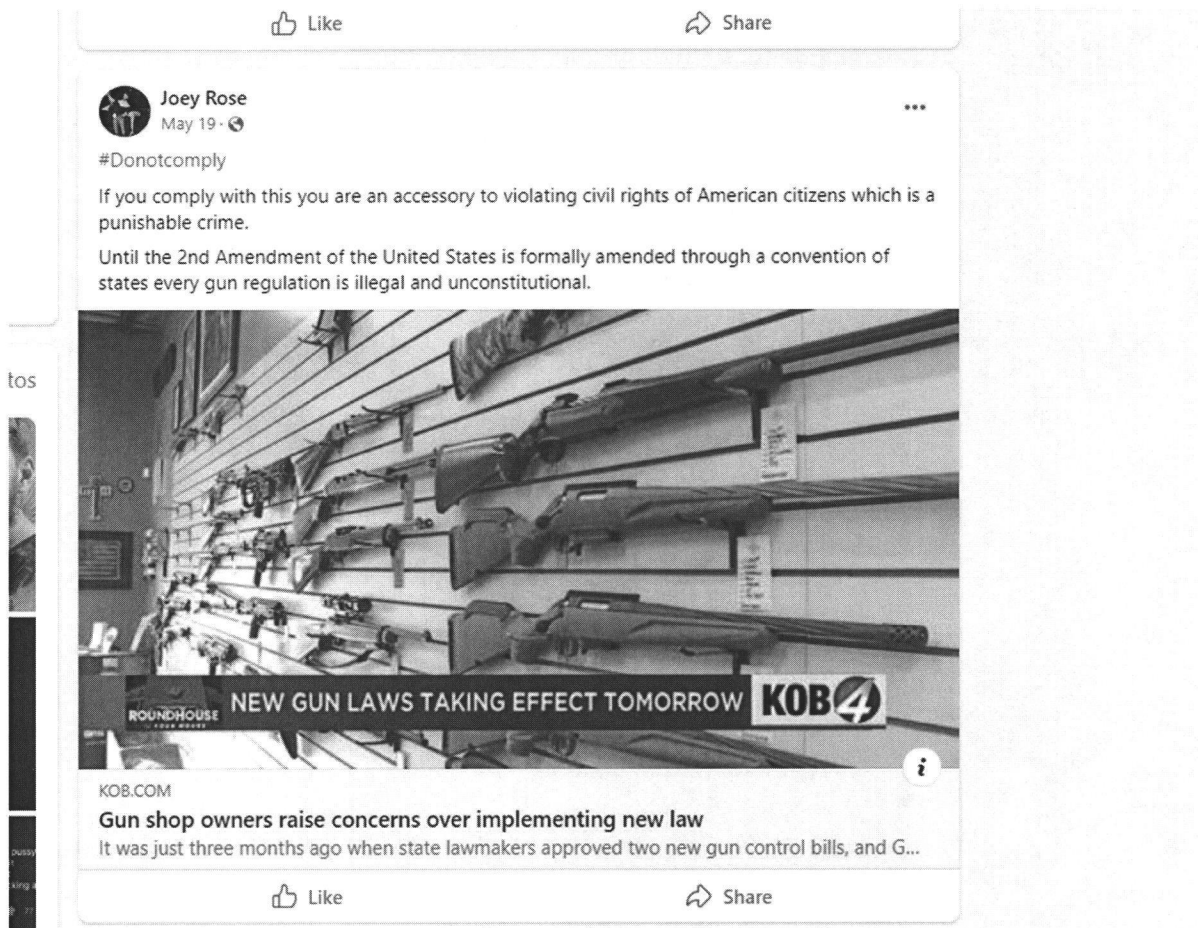
10. On June 20, 2024, FBI agents requested that Comcast voluntarily disclose, pursuant 18 U.S.C. § 2702, subscriber information for Comcast subscribers associated with the above-mentioned IP address. Comcast disclosed that the subscriber information associated with 2601:08c1:8280:5500:a5ad:d263:1277:79a5 was Joseph Rose, associated with the PREMISES on White Sands Missile Range and phone number 210-913-9272.

11. On June 20, 2024, I observed a driver's license photograph of Joseph Rose. On the same date, I observed the multiple photographs and videos posted on the Facebook account Joey.Rose.77. Based on my training and experience, I could reasonably conclude that the person on the Facebook account Joey.Rose.77 is the same person in the driver's license photograph Joseph Rose.

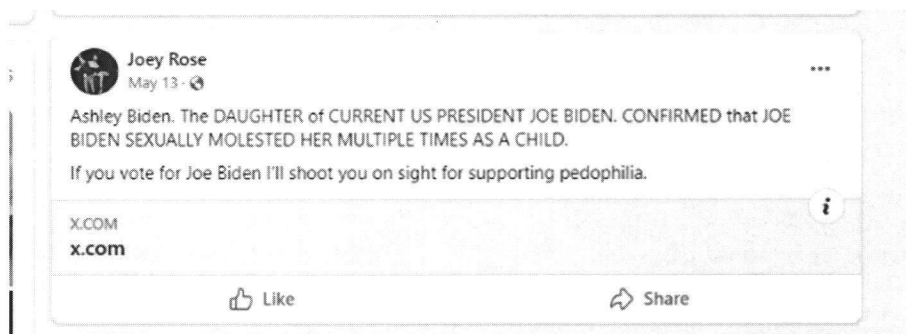
12. Based on my training and experience, I noted multiple instances on Joseph Rose's Facebook account that show Joseph Rose is pervasive in his threats and has a disdain for following laws.

13. While looking at Facebook account Joey.Rose.77, I noted photographs of Joseph Rose open carrying a pistol on his person. FBI agents ran checks with Army CID, and they had no firearms registered to him, which is a requirement for living on White Sands Missile Range. Additionally, I observed a post that stated [sic.] “#Donotcomply If you comply with this you are an accessory to violating civil rights of American citizens which is a punishable crime. Until the 2<sup>nd</sup> Amendment of the United States is formally amended through a convention of states every gun regulation is illegal and unconstitutional.” This post was regarding a new gun law in May

2024 and is shown below.



14. While looking at Facebook account Joey.Rose.77, I noted previous threatening posts, including one from May 11, 2024 stating in part [sic] “If you vote for Joe Biden I’ll shoot you on sight for supporting pedophiles.”





15. On June 20, 2024, Army CID informed FBI agents that they wanted to debar Joseph Rose from White Sands Missile Range. Army CID informed FBI agents that they canceled two trainings that were previously scheduled for June 20, 2024, after hearing of the threat on Facebook account Joey.Rose.77 due to fear of Joseph Rose having access to harm federal employees who would be on base for the trainings.

#### THE PREMISES

16. Based on the foregoing, on June 20, 2024, I sought, and the Honorable United States Magistrate Judge Gregory J. Fouratt approved, a warrant for the arrest of Joseph Rose. Based on the information contained in this affidavit, it is reasonable to believe that Joseph Rose resides at the PREMISES, and also that the threats sent by Rose were sent from the PREMISES. I therefore believe there is probable cause to search the PREMISES for Rose, and for any electronic devices which could have been used to send the threats, to include computers as described in the following section.

#### COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As referred to herein, the term “computers” takes its meaning from 18 U.S.C. § 1030(e)(1), and should thus be understood to include desktop computers, laptops, tablet computers, mobile devices, and other such devices.

18. *Probable cause.* I submit that there is probable cause to believe those records sought in Attachment B will be stored on THE DEVICES, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on THE DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of



session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic

and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to plan and execute a fraudulent scheme, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.



CONCLUSION

21. Based on the aforementioned information and investigation, I submit that probable cause exists to search THE PREMISES, as more particularly described in Attachment A and to seize the items described in Attachment B.

**This affidavit reviewed by AUSA Sarah Davenport**

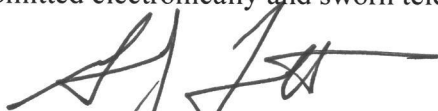
Respectfully submitted,



---

Danielle Oriatti  
Special Agent  
Federal Bureau of Investigation

Submitted electronically and sworn telephonically to me on June 20, 2024



---

Honorable Gregory J. Fouratt  
UNITED STATES MAGISTRATE JUDGE